IPhone Digital Forensic Challans and Issues

- ***Dr. Mahala Elzain Beraima Ahmed***

*assistant professor of Computer Science, Faculty of **C**omputer **S**cience and **I**nformation **T**echnology, **W**hite **N**ile **S**tate, Kosti, **S**udan*
Email:mahalaelzain2020wnu@gmail.com –mob (+249903280421)

- ***Dr. Mokhtar Mohammed***

***U**niversity of **E**limam **E**lmahdi- **f**aculty of Computer **S**cience and **I**nformation **T**echnology, **W**hite **N**ile **S**tate, Kosti **S**udan*
Email:mokhtar201328@gmail.com –mob (+249912948584)

Abstract:

Nowadays mobile phone and other handheld devices are in all the places. iPhone is having high security when compared to other Smartphone like MI, Samsung, Nokia, etc. With the continued to increase iPhone, curre ntly come with a wide range of software application, new technologies, and OS (Operating System). Therefore it becomes complicated for a forensic researcher to inspect the (evidence) proof from an iPhone proper intelligence of forensic equipment and their features are mobile forensic analysis and different types of equipment for mobile forensics and the final section of the manuscript presents the exploratory results of the tool IMYFONE D-BACK.

Keywords: *mobile phone, iPhone, IMYFONE D-BACK, forensic.*

1. INTRODUCTION

"Digital forensics is a division of forensic science focused on recovery and analysis of artifacts found on digital devices. Any equipment that storing data (E.g. Macintosh, Macbook, iPhone, Flash drives, Micro SD cards or External Hard-Disks) are within the ambit of digital forensics" [15].

Today's Smartphones such as the Apple iPhones [17] and a bulk variety of smartphone [18] are compact forms of powerful computers with high work involving nearly a Multi-core CPUs, GB of storage, and improved communication facilities such as software assisted GPS. As new features and applications are integrated into Smartphone amount of data stored on the devices is always growing. Smart application business has twisted the Smartphone into handy data carriers, and they keep follow of almost all moves of the user. Prevalence of Smartphone in everyday lives had led to their popularity in daily crimes. Thus the digital information acquired from smart devices has become one of the prime sources of proof for investigating the problems pertained to data acquisition.

In this context, the term "Smart Devices" refers to a broad spectrum of devices which have communication facilities and storage facility for digital data. There are international guidelines for the acquisition and examination of smart devices that are primarily targeted towards the preservation and non-contamination of digital data in smart devices.

The best instance of Smartphone used as a terror missile to finish the crime is the Mumbai terrorist ambush in 2008 [20]. The terrorist has taken the full benefit of being a part of the Smartphone generation. They connected electronically through smartphones to each other and with their controllers at every stage of their operation. This attack is not the first time that Smartphone are used, but the way they were performed is important and revealing. In such cases, a large amount of data can be extracted and used as forensic proof from these devices. The mobile devices evolved at an explosive rate. There are many hardware and software components used in this industry. The data quantities which can be stored on modern mobile devices are enormous. Application specific data may be stored on mobile devices. The investigation method and tool used to communicate with the mobile device can often invalidate the proof in court because it can affect the integrity and repeatability of the proof [5]. Forensically sound is the terms used to approve the use of specific forensic technology or methodology in the digital forensic circles.

The fundamental concept of sound forensic examination of digital proof is that the original proof is not altered. With mobile devices, this is extremely difficult. Most forensics required a duplex channel of communication with the mobile device and therefore the device cannot be protected against writing during forensic acquisition. Other methods of acquiring proof may include replacing the bootloader software on the mobile device or replacing a chip to facilitate access to proof.

When changing the device, the process and the resulting change need to be validated and documented. As with any collection of proof, failure to follow the proper procedure during the examination may lead to the loss or damage to proof or make it as inadmissible in court. All these challenges makes difficult to use digital forensic analysis tools on mobile devices. It should be noted that ISO 27037 specification “Detection, collection and/or acquisition and preservation guidelines for digital evidence” (2012) defines methods and techniques accepted in many jurisdictions in digital forensics [12].

2. SMARTDEVICES & PROOF PRESERVATION

The collection of proof at the crime site shall include the preservation of the state of the devices:

1. A switched ON device must be kept on
2. It must be protected from external WiFi signals while maintaining the state of the WiFi status of the phone.
3. It should be isolated from telecommunication signals (like 4G, LTE, etc.)
4. GPS signals must be isolated.
5. IT battery should be charged (preferably at the same level of the battery)

If a mobile device on a crime site is not isolated from all such factors listed above, it will become very easy for the attacker to gain access to the device and lock or destroy all proof in it. This is usually done the facilities provided by the iphone, such as iOS from Apple. Figure 1 Shows how easy it is for the owner (the criminal in this case) to remotely locate, access, lock, and delete a typical iPhone.

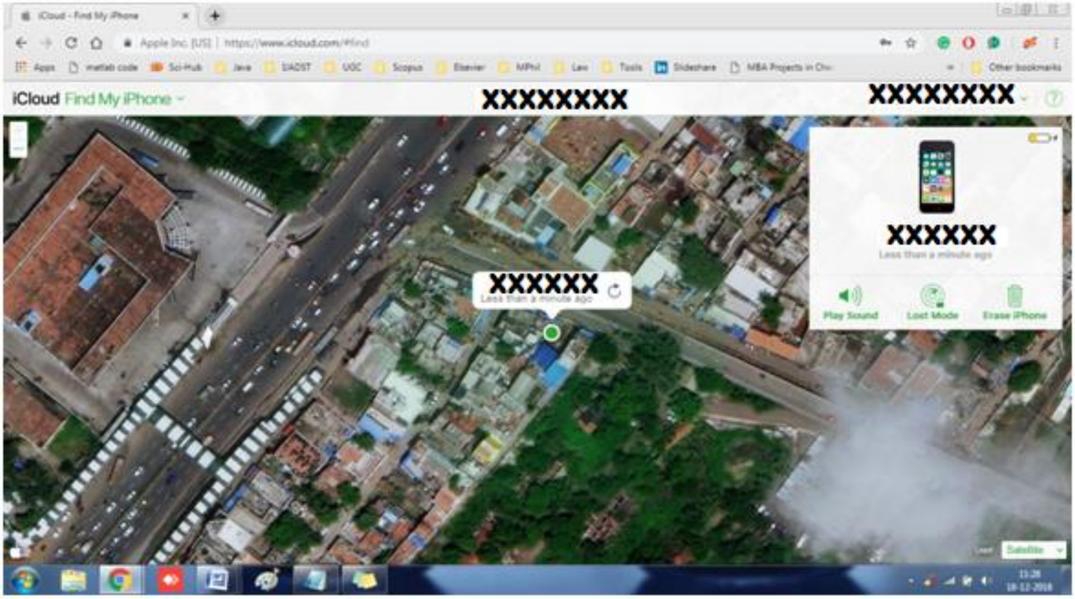


Fig 1: Remotely Track and erase iPhone with iCloud

3. WORKFLOW

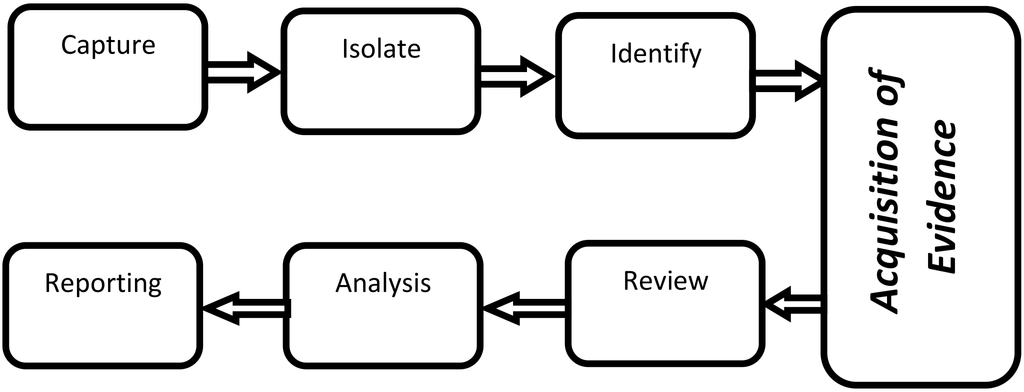


Fig 2: Workflow of mobile forensics

The digital forensic of iPhone process (Based on the Figure 2) can be divided into several categories,

3.1. CAPTURE, ISOLATE AND IDENTIFY

At the time of the seizure, it is important to document with photos the various mobile state information –including not to the current (on or off) and the locking status, presence or absence of Memory Cards, etc. All hardware and software accessories including cables, chargers, subscriber identity module (SIM) card data, personal identification number (PIN) hints or passwords are collected as well. As already shown, it is essential to protect the device from communicating with external agencies-including phone calls (but not limited to), short message service (SMS), Wireless Fidelity (WiFi), Bluetooth and Global Positioning System (GPS).

During the collection of proof, a phone call or SMS or an email may overwrite the previous ones. An iPhone which can be accessed via the internet can easily be remotely wiped. Thus, the following equipment, such as a faraday bag and/or radio jammer, must be used to prevent all electromagnetic communication with the device. Phone features such as “Airplane mode” can also be used many times to prevent radio communications to foreign countries. Functions such as “stay awake” can also be used to keep the iPhone unlocked (display turned on).

3.2. ACQUISITION OF PROOF

Data extraction from SIM requires hardware tools such as PC/SC Reader that acquires GSM 11.11 data on the device’s internal memory (E.g. a Memory Chip) can be copied bit by bit from a whole physical store. This allows the deleted files and any remaining data to be examined, which would otherwise not be accounted for. The other copying method for logical entities such as files and directories may prove to be a simpler method during the examination. There are various software tools for extracting data from the memory.

Specialized forensic software products can be automated or generic file viewers, like hex editors, are available. Some specialist tool includes access the data for memory image analysis. Since one tool cannot extract all the information, it is often recommended that two or more tools be used. When the acquisition becomes more forensically sound, tools become more costly, analyses are longer and tools require more training.

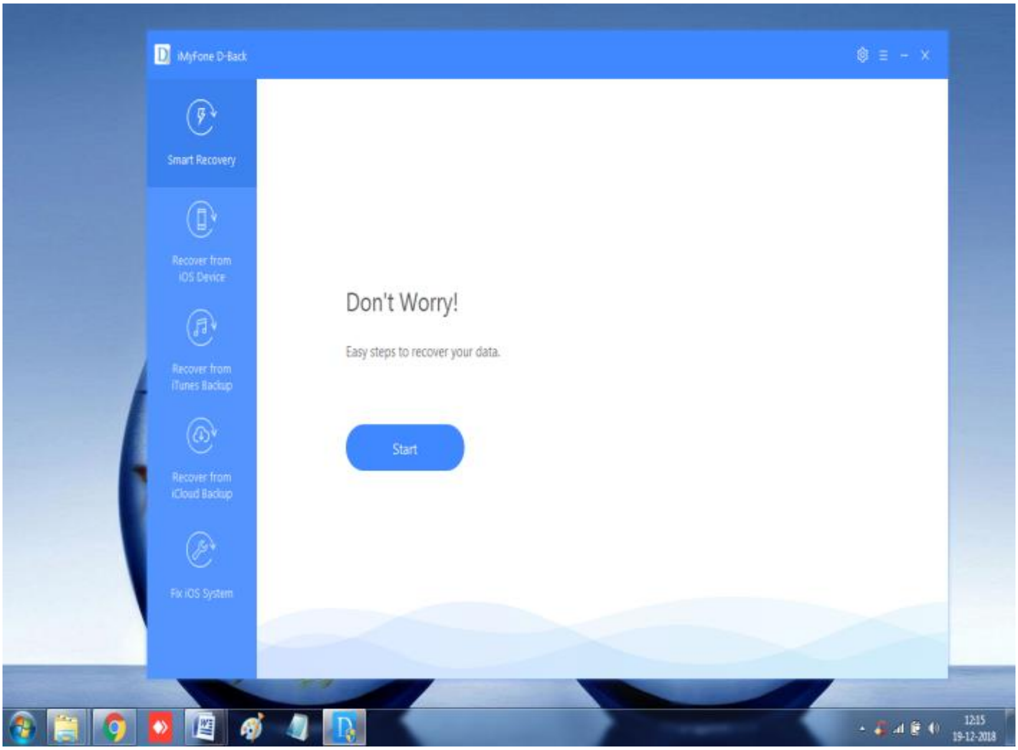
3.3. REVIEW, ANALYSIS AND REPORTING

1. **Logical acquisition:** A bitwise copy of logical storage objects such as directories and logical storage files (E.g. A partition of the file system).

2. **Manual acquisition:** This method uses the mobile User Interface (UI) to scan the contents of the iPhone’s memory.
3. **Metadata acquisition of the system file:** When user data is organized in a database, it is called META data. Such META databases may provide valuable information on the use of the device; E.g. Call is a simple SQLite database file
4. in iOS.
5. **Physical acquisition:** It is the binary dump of the entire file system. This may contain information on existing or deleted system file objects.
6. **Acquisition of brute:** it is used to extract passwords or PINs. Brute force tools are connected data as a password or PIN until successful. It takes time but often depends on the complexity of the original password or PIN.

On iPhone’s, the acquisition of proof is greatly simplified once the IMYFONE D-(IMDB) with iTunes is enabled. This option is probably the best tool for the forensic surveyor when extracting data from an iOS, without affecting or altering the telephone status. You can find this option in settings development of nearly all iPhones.

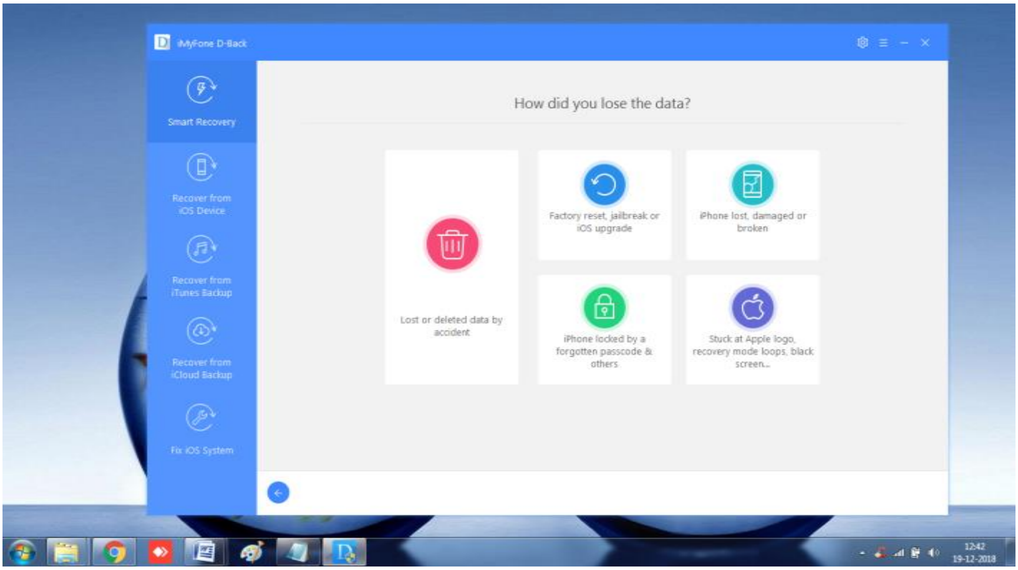
iOS software development kit (ISDK) includes [19] this powerful IMDB tool to communicate via USB and WiFi with the IMDB-enabled iPhone. Most of the above information can be accessed from the desktop of the investigator using IMDB. Please note that 99 percent of IMDB’s Features can be used to access the iphone without root, making IMDB one of the best tools for collecting and analyzing iPhone forensic as shown in Figure 3a, 3b.



Don't Worry!

Easy steps to recover your data.

Fig 3a: User Interface of IMDB



How did you lose the data?

Lost or deleted data by accident

Factory reset, jailbreak or iOS upgrade

iPhone lost, damaged or broken

iPhone locked by a forgotten passcode & others

Stuck at Apple logo, recovery mode loops, black screen...

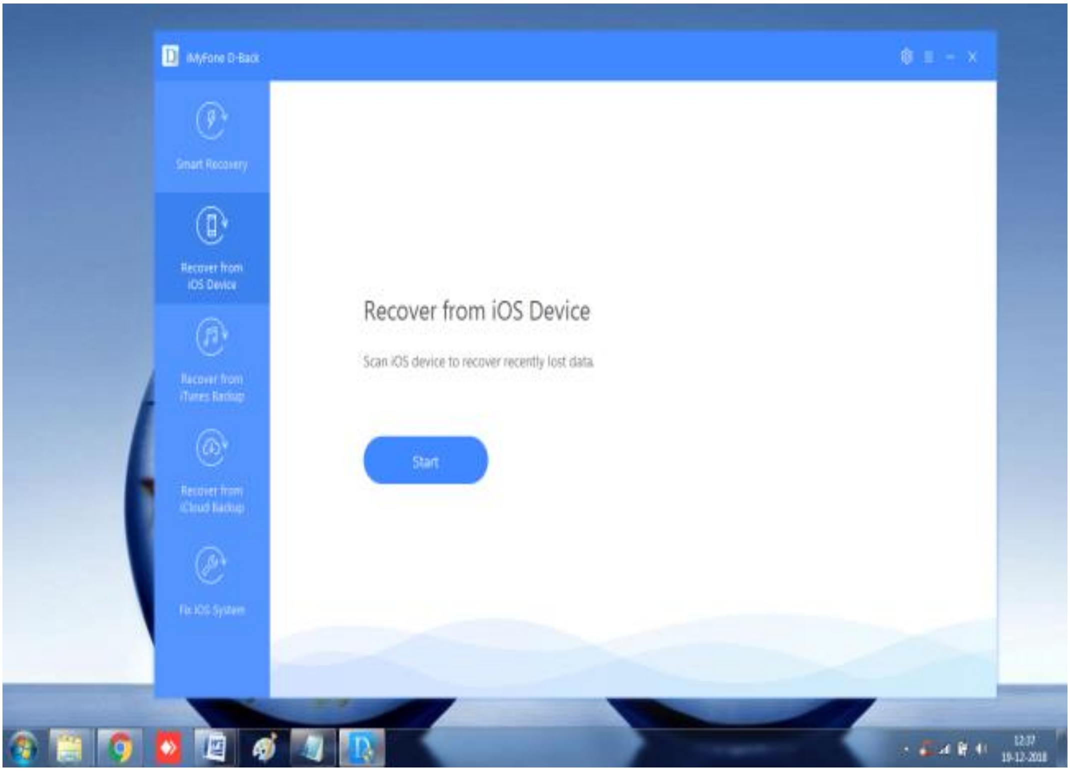
Fig 3b: Recover options in IMDB

FEATURES IN IMDB

IMDB is the best tool for forensic analysis.

1. Recover from iOS device

This mode can be used to recover the recently deleted data from the iOS devices Via USB device as shown in Figure 4.



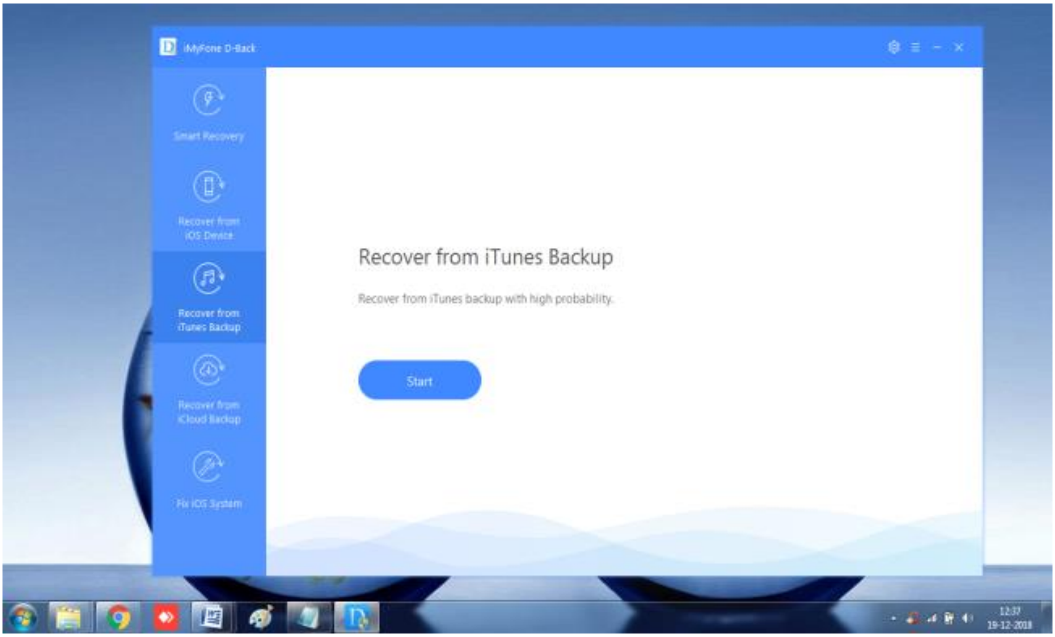
Recover from iOS Device

Scan iOS device to recover recently lost data

Fig 4: Recover data from iOS device in IMDB

2. Recover from iTunes backup

This mode can be used to recover the recently deleted data from the iTunes via cloud with high probability as shown in Figure 5.

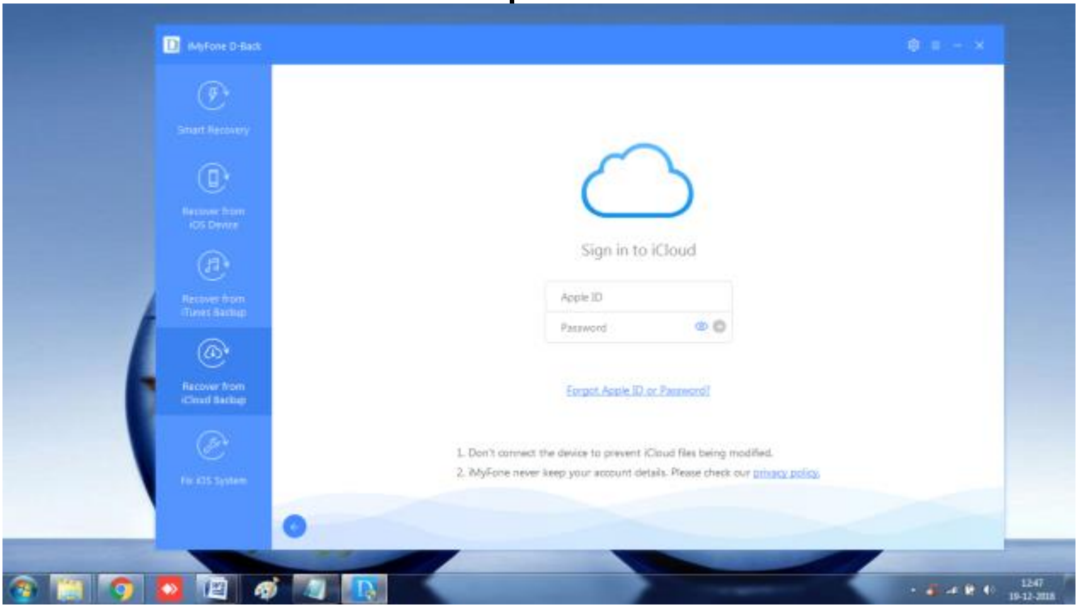


Recover from iTunes Backup

Recover from iTunes backup with high probability.

Fig 5: Recover data from iTunes in IMDB

3. Recover from iCloud backup



Sign in to iCloud

Apple ID

Password

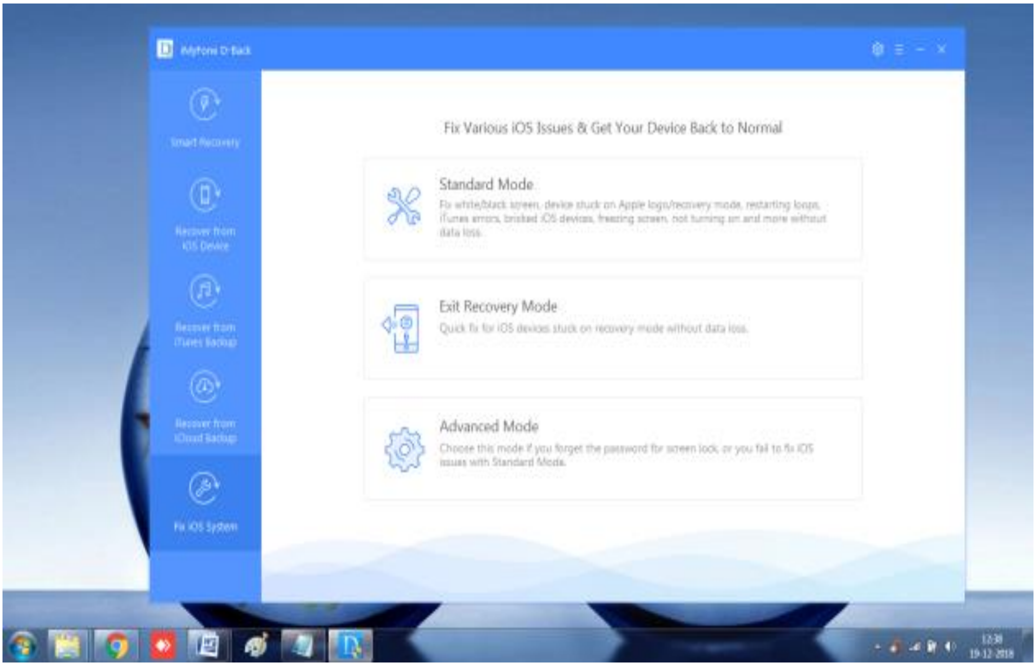
Forgot Apple ID or Password?

1. Don't connect the device to prevent iCloud files being modified.
2. iMyFone never keep your account details. Please check our privacy policy.

Fig 6: Recover data from iCloud in IMDB

7. FIX iOS SYSTEM

Fix various iOS issues & get your devices to normal with the help of IMDB as shown in Figure 7.



Fix Various iOS Issues & Get Your Device Back to Normal

Standard Mode
Fix white/black screen, device stuck on Apple logo/recovery mode, restarting loops, iTunes errors, bricked iOS devices, freezing screen, not turning on and more without data loss.

Exit Recovery Mode
Quick fix for iOS devices stuck on recovery mode without data loss.

Advanced Mode
Choose this mode if you forget the password for screen lock, or you fail to fix iOS issues with Standard Mode.

Fig 7: Fix iOS device issues in IMDB

ii. Standard mode

Fix the white/black screen, device stuck on apple logo/recovery mode, restarting loops, iTunes errors, bricked iOS devices, freezing screen, not turning on and more without data loss.

ii. Exit recovery mode

Quick fix iOS mode if you forgot the password for screen lock, or you fail to fix iOS issues with standard mode.

iii. Advanced mode

Choose this mode if you forgot the password for screen lock, or you fail to fix iOS issues with standard mode.

RESULT AND ANALYSIS

Once proof is acquired (as described above in many forms), the following are the most common logical entities which are the potential proof source in a mobile device. i.e. These are the possible logical entities to be investigated in a mobile device as shown in Figure 7a, Figure 7b, Figure 7c, Figure 7d, figure 7e, Figure 7f, Figure 7g, Figure 7h, Figure 7i, Figure 7j, Figure 7k, Figure 7l, Figure 7m, Figure 7n.

- Message
- Call history
- Contact
- Whatsapp
- Wechat, qq viber, kik
- Skype
- Line
- Photo
- Video
- App photo
- App video
- Note
- Voice memo
- Safari bookmark
- Calendar & reminder
- Safari history

Two types of forensic investigations are possible with the proof data.

1. A crime has already taken place and the identity of the criminal (E.g. hacking incident) is unknown.

2. The crime and the criminal are both known (E.g. child pornography investigation).

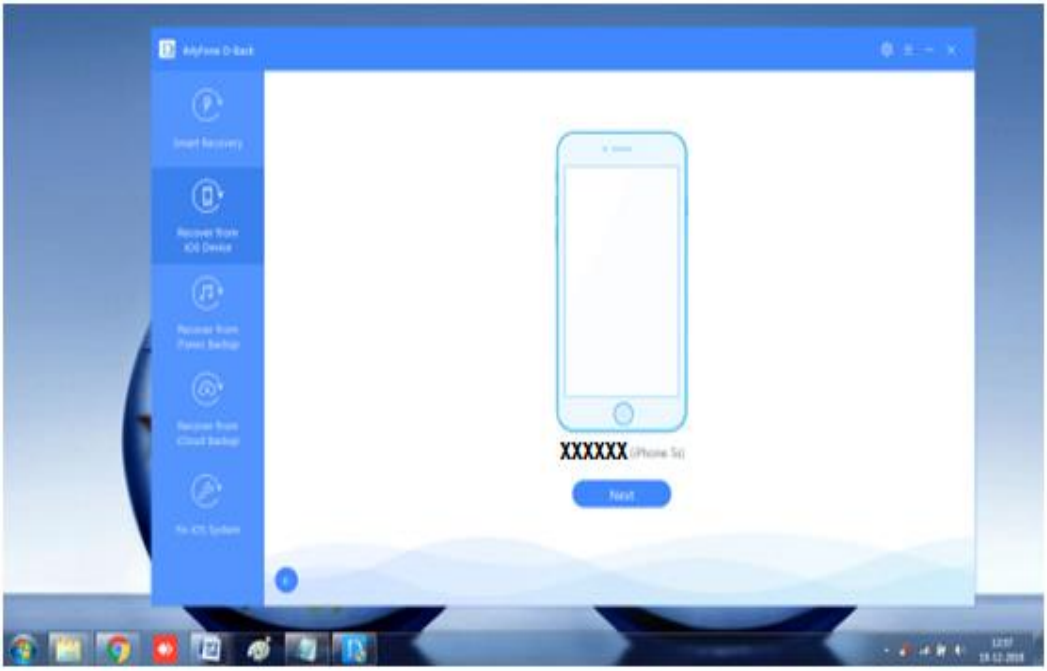
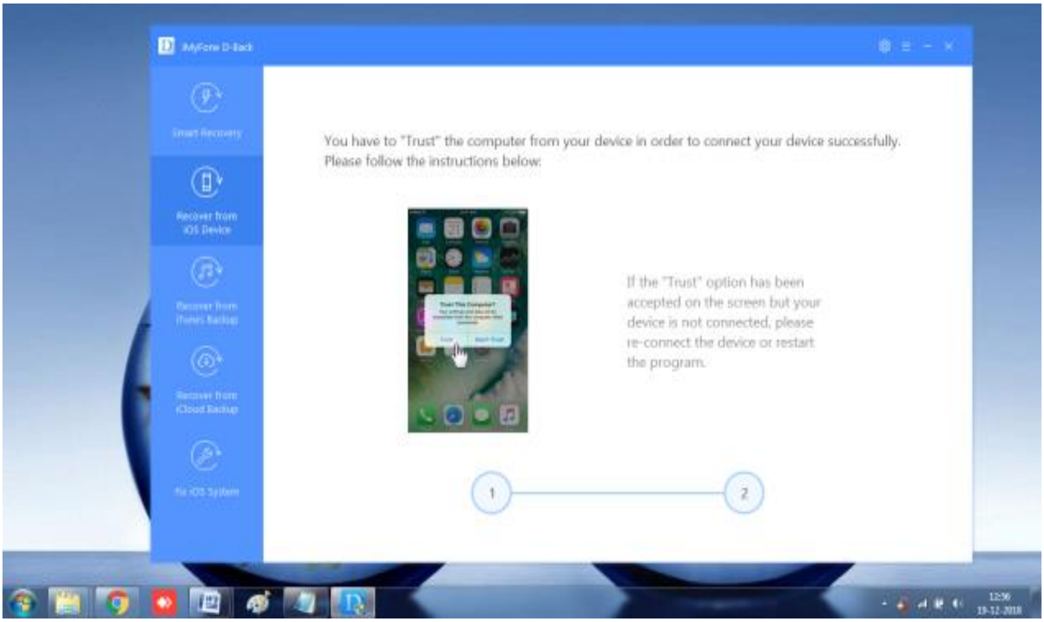


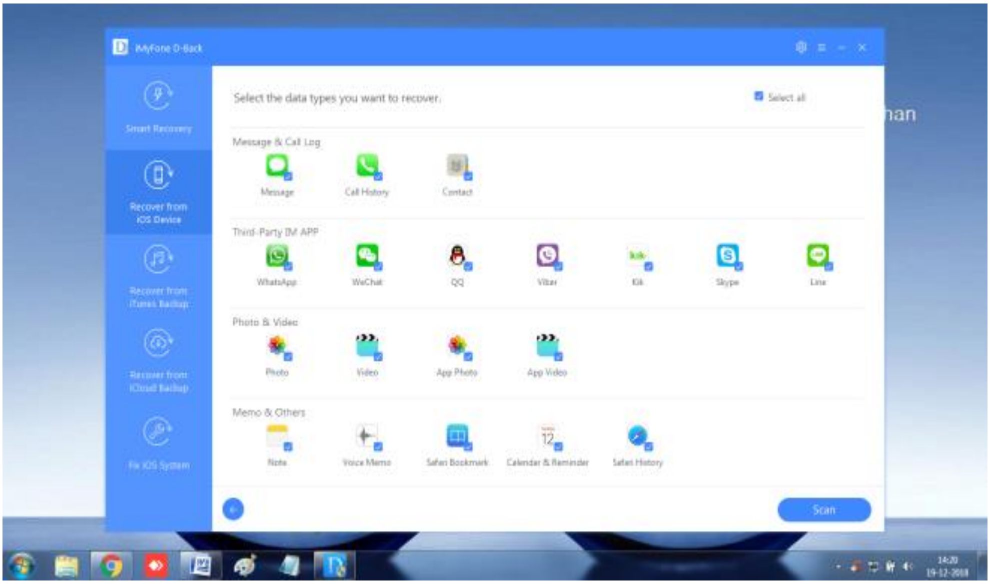
Fig 7a: Connecting iPhone in IMDB



You have to "Trust" the computer from your device in order to connect your device successfully. Please follow the instructions below:

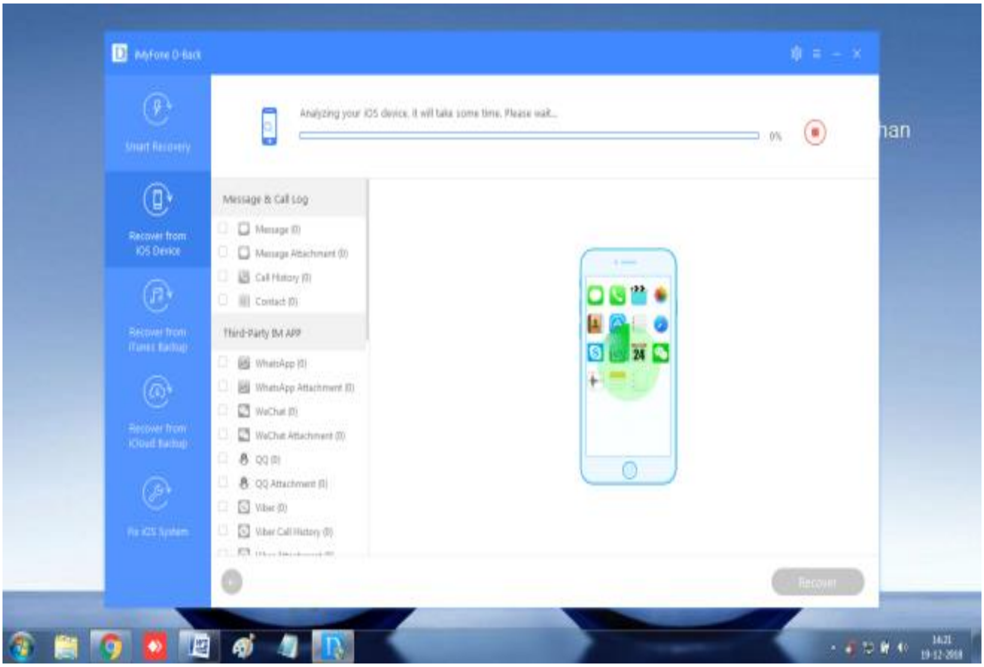
If the "Trust" option has been accepted on the screen but your device is not connected, please re-connect the device or restart the program.

Fig 7b: Establishing Connection between iPhone & IMDB



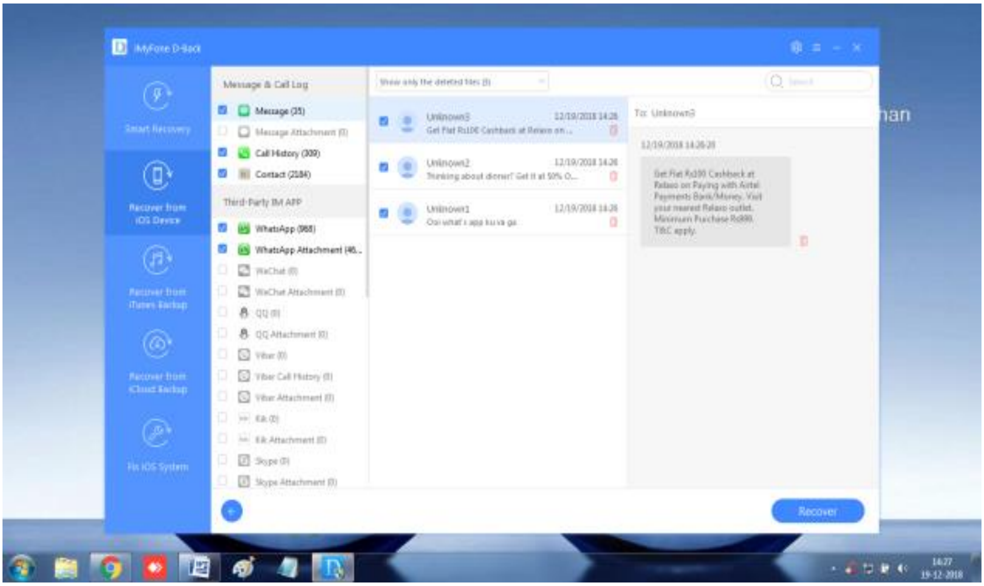
Select the data types you want to recover.

Fig 7c: Recoverable data's from iPhone 5s



Analyzing your iOS device, it will take some time. Please wait...

Fig 7d: Data recovering from iPhone



☑ Unknown3 12/19/2018 14:26
Get Flat Rs100 Cashback at Relaxo on...

☑ Unknown2 12/19/2018 14:26
Thinking about dinner? Get it at 50% O...

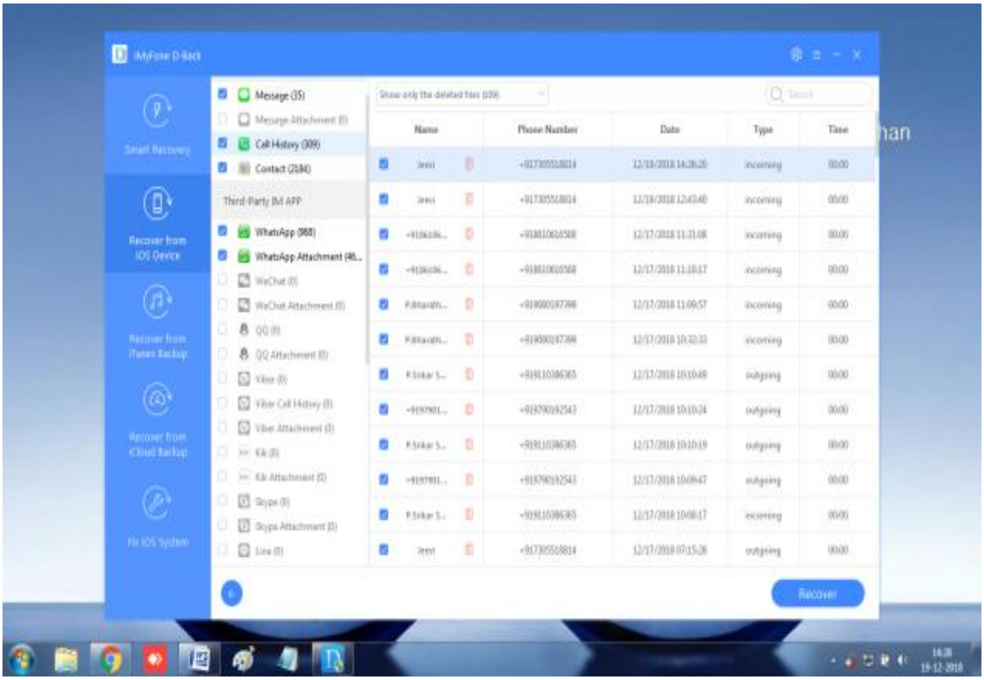
☑ Unknown1 12/19/2018 14:26
Ooi what's app ku va ga

To: Unknown3

12/19/2018 14:26:20

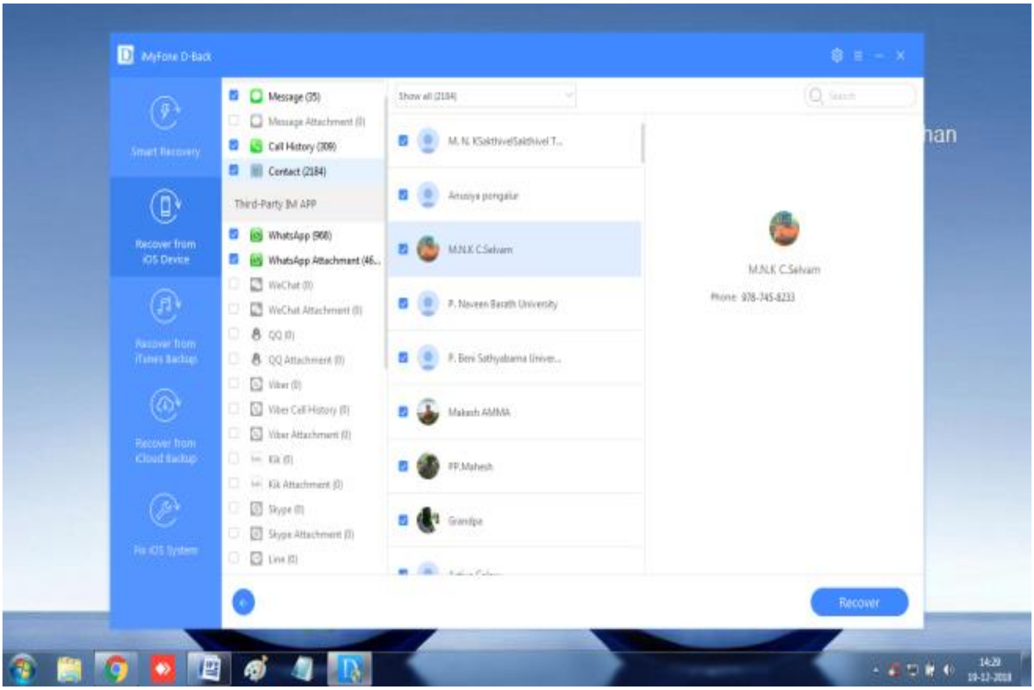
Get Flat Rs100 Cashback at Relaxo on Paying with Airtel Payments Bank/Money. Visit your nearest Relaxo outlet. Minimum Purchase Rs999. T&C apply.

Fig 7e: Message history



	Name	Phone Number	Date	Type	Time
☑	Jeevi	+917305518814	12/19/2018 14:26:20	incoming	00:00
☑	Jeevi	+917305518814	12/19/2018 12:43:40	incoming	00:00
☑	+9188106...	+918810616568	12/17/2018 11:21:08	incoming	00:06
☑	+9188106...	+918810616568	12/17/2018 11:18:17	incoming	00:00
☑	P.Bharath...	+919080197398	12/17/2018 11:09:57	incoming	00:00
☑	P.Bharath...	+919080197398	12/17/2018 10:32:32	incoming	00:00
☑	P.Sekar S...	+919110386365	12/17/2018 10:10:48	outgoing	00:00
☑	+9197901...	+919790192543	12/17/2018 10:10:24	outgoing	00:00
☑	P.Sekar S...	+919110386365	12/17/2018 10:10:19	outgoing	00:00
☑	+9197901...	+919790192543	12/17/2018 10:09:47	outgoing	00:00
☑	P.Sekar S...	+919110386365	12/17/2018 10:08:17	incoming	00:06
☑	Jeevi	+917305518814	12/17/2018 07:15:26	outgoing	00:00

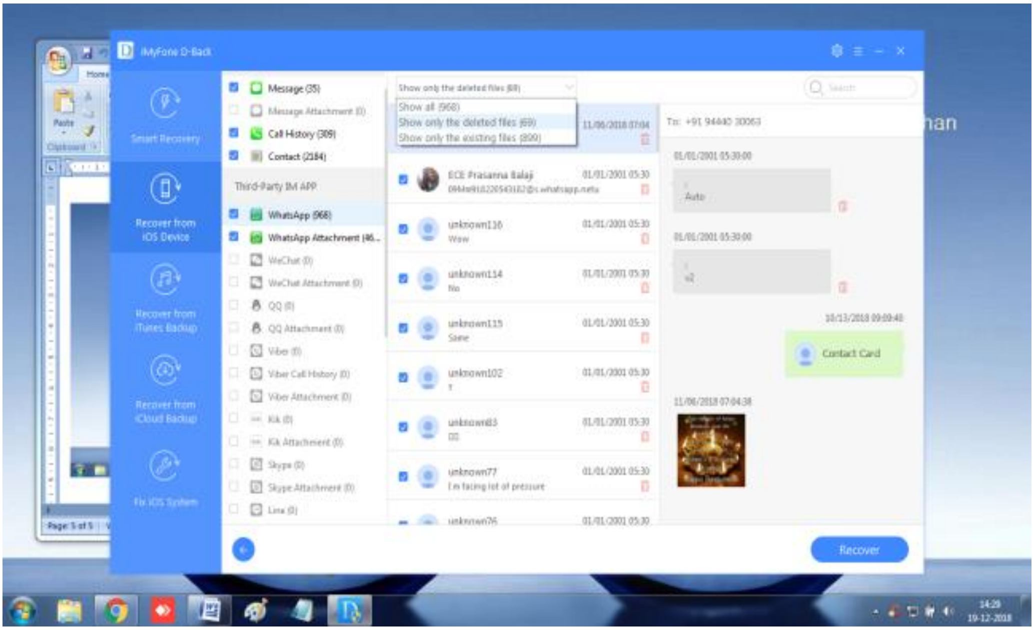
Fig 7f: Call history



M. N. KSakthivelSakthivel T...
Anusiya pongalur
M.N.K C.Selvam
P. Naveen Barath University
P. Beni Sathyabama Univer...
Makesh AMMA
PP.Mahesh
Grandpa

M.N.K C.Selvam
Phone: 978-745-8233

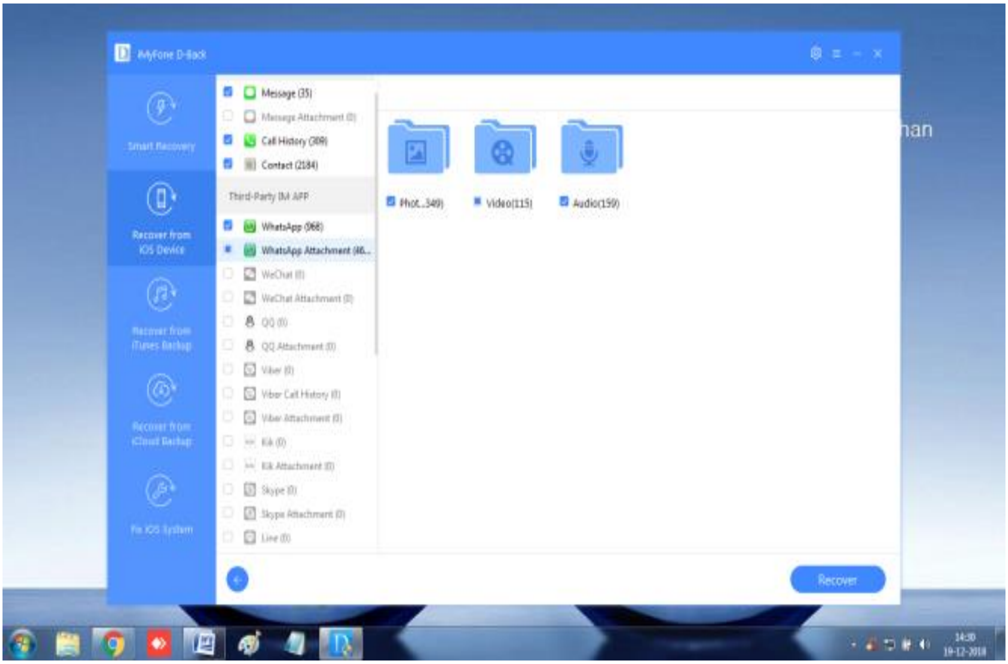
Fig 7g: Available Contacts



11/06/2018 07:04
ECE Prasanna Balaji 01/01/2001 05:30
unknown116 01/01/2001 05:30
Wow
unknown114 01/01/2001 05:30
No
unknown115 01/01/2001 05:30
Sane
unknown102 01/01/2001 05:30
unknown83 01/01/2001 05:30
unknown77 01/01/2001 05:30
I m facing lot of pressure
unknown76 01/01/2001 05:30

To: +91 94440 30063
01/01/2001 05:30:00
Auto
01/01/2001 05:30:00
10/13/2018 09:09:40
Contact Card
11/06/2018 07:04:38

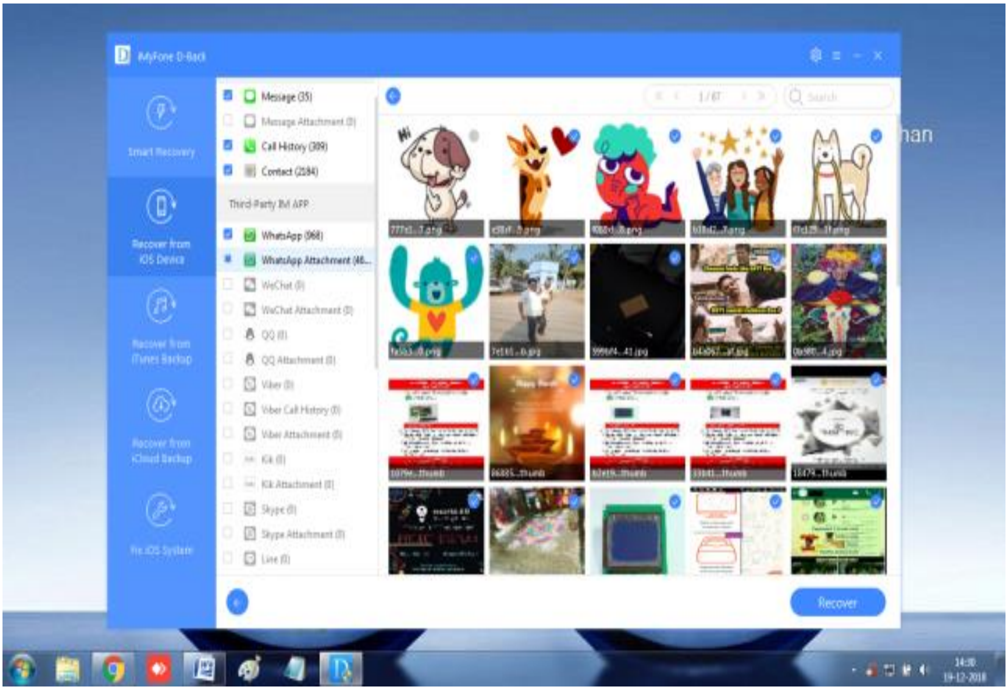
Fig 7h: Whatsapp Message



☑ Message (35)
□ Message Attachment (0)
☑ Call History (309)
☑ Contact (2184)
Third-Party IM APP
☑ WhatsApp (968)
■ WhatsApp Attachment (46...
□ WeChat (0)
□ WeChat Attachment (0)
□ QQ (0)
□ QQ Attachment (0)
□ Viber (0)
□ Viber Call History (0)
□ Viber Attachment (0)
□ Kik (0)
□ Kik Attachment (0)
□ Skype (0)
□ Skype Attachment (0)
□ Line (0)

☑ Phot...349) ■ Video(115) ☑ Audio(159)

Fig 7i: Whatsapp Attachments



☑ Message (35)
□ Message Attachment (0)
☑ Call History (309)
☑ Contact (2184)
Third-Party IM APP
☑ WhatsApp (968)
■ WhatsApp Attachment (46...
□ WeChat (0)
□ WeChat Attachment (0)
□ QQ (0)
□ QQ Attachment (0)
□ Viber (0)
□ Viber Call History (0)
□ Viber Attachment (0)
□ Kik (0)
□ Kik Attachment (0)
□ Skype (0)
□ Skype Attachment (0)
□ Line (0)

Fig 7j: Available & Deleted Whatsapp attachment Photos

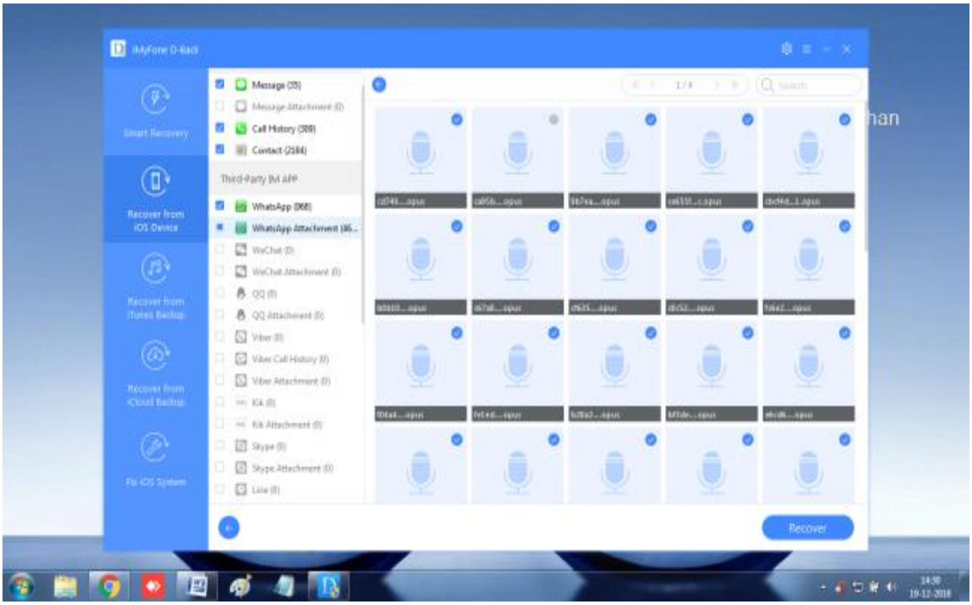


Fig 7k: Available & Deleted Whatsapp attachment Videos

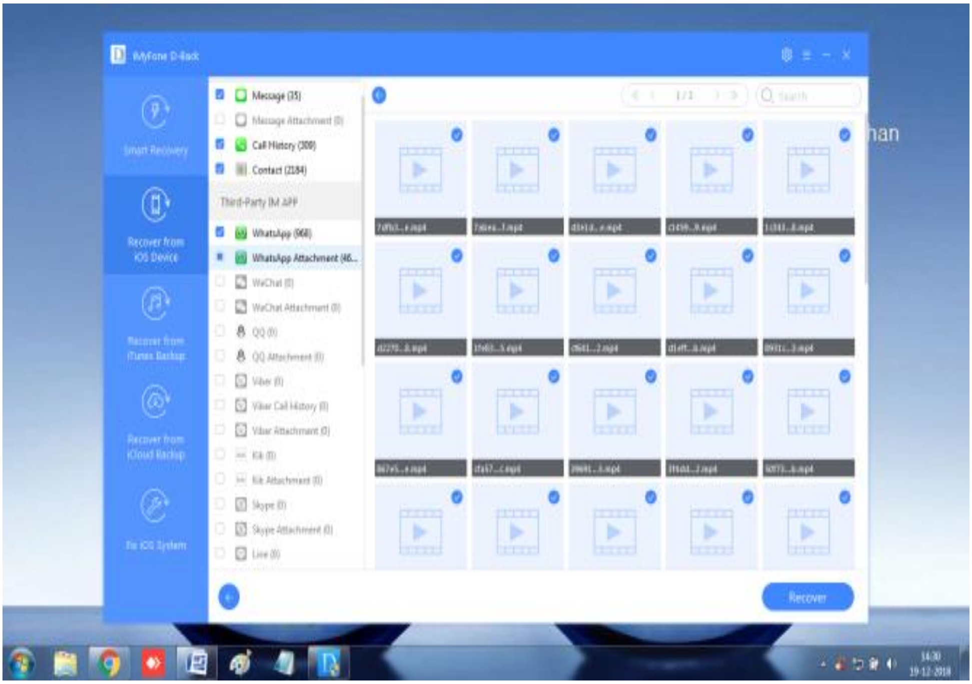
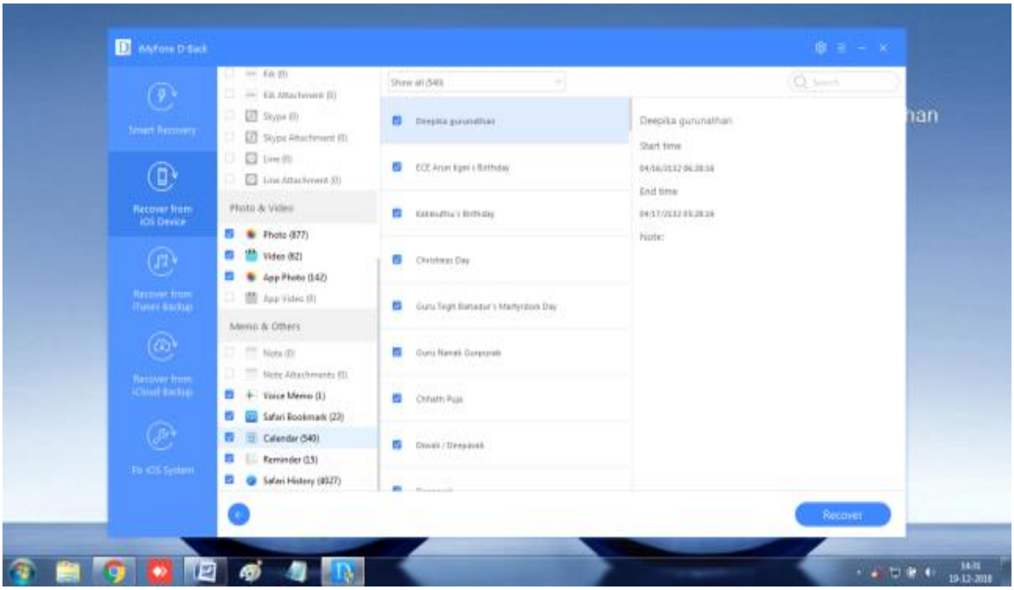


Fig 7l: Available & Deleted Whatsapp attachment Audios



☑ Deepika gurunathan

☑ ECE Arun Ilgel's Birthday

☑ Kakeluthu's Birthday

☑ Christmas Day

☑ Guru Tegh Bahadur's Martyrdom Day

☑ Guru Nanak Gurpurab

☑ Chhath Puja

☑ Diwali / Deepavali

Deepika gurunathan

Start time

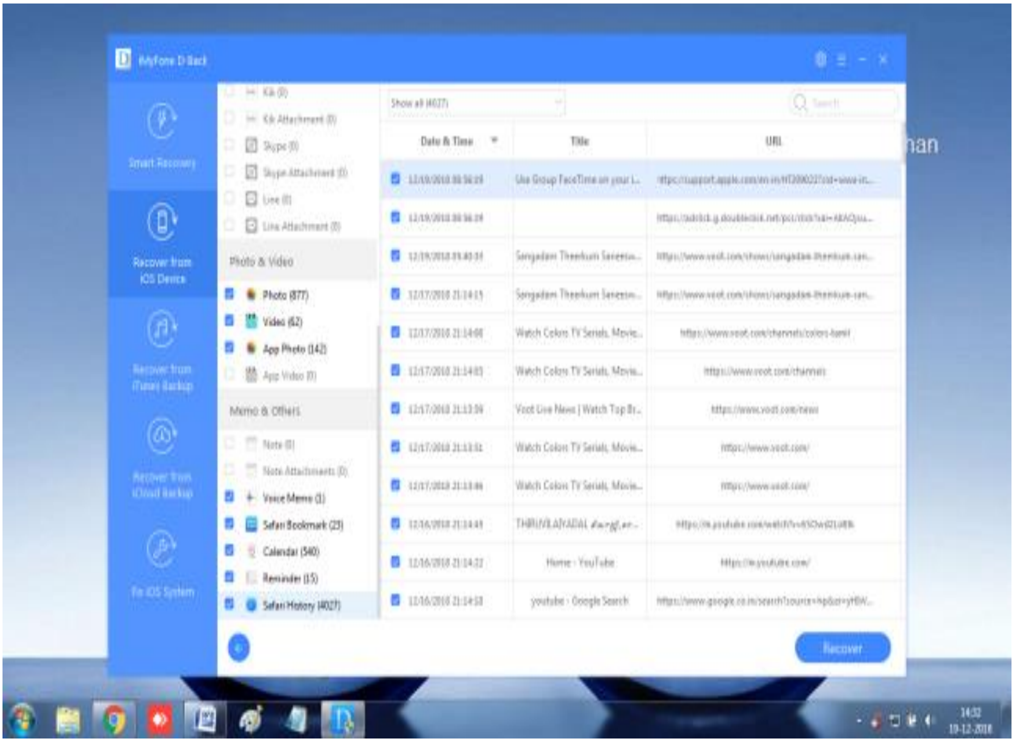
04/16/2132 06:28:16

End time

04/17/2132 05:28:16

Note:

Fig 7m: Available and deleted Calendar details



	Date & Time	Title	URL
☑	12/19/2018 08:56:28	Use Group FaceTime on your i...	https://support.apple.com/en-in/HT209022?cid=www-in...
☑	12/19/2018 08:56:28		https://adclick.g.doubleclick.net/pcs/click?xai=AKAOjsu...
☑	12/19/2018 09:40:16	Sangadam Theerkum Saneesw...	https://www.voot.com/shows/sangadam-theerkum-san...
☑	12/17/2018 21:14:15	Sangadam Theerkum Saneesw...	https://www.voot.com/shows/sangadam-theerkum-san...
☑	12/17/2018 21:14:08	Watch Colors TV Serials, Movie...	https://www.voot.com/channels/colors-tamil
☑	12/17/2018 21:14:03	Watch Colors TV Serials, Movie...	https://www.voot.com/channels
☑	12/17/2018 21:13:59	Voot Live News | Watch Top Br...	https://www.voot.com/news
☑	12/17/2018 21:13:51	Watch Colors TV Serials, Movie...	https://www.voot.com/
☑	12/17/2018 21:13:46	Watch Colors TV Serials, Movie...	https://www.voot.com/
☑	12/16/2018 21:14:49	THIRUVILAIYADAL [illegible]...	https://m.youtube.com/watch?v=R5Owd21u8k
☑	12/16/2018 21:14:22	Home - YouTube	https://m.youtube.com/
☑	12/16/2018 21:14:50	youtube - Google Search	https://www.google.co.in/search?source=hp&ei=yHBW...

Fig 7n: Safari history

Prepared against the background of the incident and the proof collected [6], the forensic expert can pursue the following goals:

1. Who all are involved: collect information of the people involved in crime.
2. What is the nature of the events?
3. When did the crime-related events occur?
4. Why did the delinquent commit the offense?
5. What are the tools and methods used by offenders to carry out the offense?

CONCLUSION

Mobile forensic is the digital forensic branch that acquires and analyses mobile devices to detect and retrieve digital proof. We have studied forensic literatures using iPhone and identified the methods and studies carried out in this field, regardless of the types of the system used and the few tools already in common use. In this paper, we identified the mobile forensic workflow and the methods for acquiring and documenting proof for future use.

REFERENCES

[1] Botta A, De Donato W, Persico V, Pescapé A. On the integration of cloud computing and internet of things. In Future internet of things and cloud (FiCloud), 2014 international conference on 2014 Aug 27 (pp. 23-30). IEEE.

[2] Adams RB, Hobbs V, Mann G. The Advanced Data Acquisition Model (ADAM) &58; A Process Model for Digital Forensic Practice. Journal of Digital Forensics. 2013 Jan 1;8(4):25-48.

[3] MacDermott A, Baker T, Shi Q. IoT Forensics: Challenges For The IoA Era. In New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on 2018 Feb 26 (pp. 1-5). IEEE.

[4] Grajeda C, Breitinger F, Baggili I. Availability of datasets for digital forensics–and what is missing. Digital Investigation. 2017 Aug 1; 22:S94-105.

[5] Pieterse H, Olivier M. Smartphones as distributed witnesses for digital forensics. InIFIP International Conference on Digital Forensics 2014 Jan 8 (pp. 237-251). Springer, Berlin, Heidelberg.

[6] Bennett D. The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. Information Security Journal: A Global Perspective. 2012 Jan 1;21(3):159-68.

[7] Chung H, Park J, Lee S. Digital forensic approaches for Amazon Alexa ecosystem. Digital Investigation. 2017 Aug 1; 22:S15-25.

[8] MRKAIĆ I. Android forensic using some open source tools. In The Eighth International Conference on Business Information Security (BISEC-2016), Belgrade, Serbia,, 15th October 2016.

[9] Conlan K, Baggili I, Breitinger F. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital investigation. 2016 Aug 7;18:S66-75.

[10] Gül M, Kugu E. A survey on anti-forensics techniques. Inartificial Intelligence and Data Processing Symposium (IDAP), 2017 International 2017 Sep 16 (pp. 1-6). IEEE.

[11] Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Network Security. 2011 Mar 1;2011(3):4-10.

[12] Retrieved from: Csrc.nist.gov. (2018). SP 800-101 Revision 1, Guidelines on Mobile Device Forensics | CSRC. [online] Available at: https://csrc.nist.gov/News/2014/SP-800-101-Revision-1,-Guidelines-on-Mobile-Device [Accessed 26 Dec. 2018].

[13] Roy NR, Khanna AK, Aneja L. Android phone forensic: tools and techniques. InComputing, Communication and Automation (ICCCA), 2016 International Conference on 2016 Apr 29 (pp. 605-610). IEEE.

[14] Aziz NA, Mokhti F, Nozri MN. Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone. InCyber Security, Cyber Warfare, and Digital

Forensic (CyberSec), 2015 Fourth International Conference on 2015 Oct 29 (pp. 123-128). IEEE.

[15] Sengul Dogan, Erhan Akbal. Analysis of Mobile Phones in Digital Forensics. MIPRO 2017, May 22- 26, 2017, Opatija, Croatia. IEEE.

[16] Support.apple.com. (2018). iCloud: Manage your devices in Settings on iCloud.com. [online] Available at: https://support.apple.com/kb/PH21251?locale=en_GB [Accessed 26 Dec. 2018].

[17] Adam Jansen. Digital Records Forensics:Ensuring Authenticity and Trustworthiness of Evidence Over Time. 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering. IEEE.

[18] Shams Zawoad, Ragib Hasan, and Anthony Skjellum. OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. 2015 IEEE 8th International Conference on Cloud Computing. IEEE

[19] Ezhil Kalaimannan. Smart Device Forensics - Acquisition, Analysis and Interpretation of Digital. Evidences. 2015 International Conference on Computational Science and Computational Intelligence. IEEE.

[20] Mohammad Mahfuzul Haque1, Syed Akther Hossain. National Digital Forensics Framework for Bangladesh. 2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 7-9 December 2017, Khulna, Bangladesh. IEEE.

[21] Sqlite.org. (2018). SQLite Encryption Extension: Documentation. [online] Available at: http://www.sqlite.org/see [Accessed 26 Dec. 2018].

[22] Aziz N, Mokhti F, Nozri M. Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone. 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec). 2015.

[23] Salama U. Smart Forensics for the Internet of Things (IoT) [Internet]. Security Intelligence. Security Intelligence; 2017 [cited 2018Dec26]. Available from:

[24] https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/Rao VV, Chakravarthy A. Forensic analysis of android mobile devices. 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE). 2016;

[25] Rao V, Chakravarthy AS. Survey on Android forensic tools and methodologies. Int. J. Comput. Appl. 2016;154:17-21.